1) Which of the following is an audit requirement?

   a) a code (e.g., a numeric error message or reason) must be attachedto the result of an audited event describing why it succeeded or failed.
   b) a system administrator must be able to obtain information regarding system activity based upon a user's identity and/or an object'ssecurity level.
   c) real-time Intrusion Countermeasure Equipment (ICE) must be used.
   d) a secondary file must exist and be used when the primary audit file becomes full.
   e) None of the above.

2) A security-relevant event is any event that:

   a) may lead to a violation of the system security policy.
   b) depicts a system fault and executes a trusted recovery.
   c) regulates the access of information.
   d) processes violations of the security policy in the system.
   e) None of the above.

3) For TCSEC classes C2 through A1, the TCSEC requires that a user'sactions be open to scrutiny by means of an audit.

   a) TRUE.
   b) FALSE.

4) Users should be notified that their actions are being audited.

   a) TRUE.
   b) FALSE.

5) Comparing audit data against which of the following would be most likelyto discern undesirable activity on a trusted system?

   a) security policy statements and profiles of individual users.
   b) individual profiles and historical audit data for that user.
   c) profiles of identified suspicious individuals and a collection offeatures such as usual login time, terminal location, etc.
   d) identified attack methods and real-time threshold alarms.
   e) TCSEC requirements and system policy.

6) The security goals of an audit mechanism include:

   a) providing user assurance that attempts to bypass the protection mechanisms are discovered and damage controlled.
   b) acting as a deterrent against attempts to bypass protection mechanisms
   c) allowing the review of patterns of access to objects.
   d) allowing the discovery of use of privileges.
   e) All of the above.

7) Misfeasors are:

a) clandestine users who are not authorized to use the system resources accessed.
b) external penetrators.
c) users masquerading by operating under another user's ID and authentication.
d) authorized users of the system and resources who misuse theirprivilege.
e) None of the above.

8) Override of human-readable output markings must be auditable at class:

a) C1.
b) C2.
c) B1.
d) All of the above.
e) None of the above.

9) Authentication information should not be audited.

a) TRUE.
b) FALSE.

10) Requiring that an action be auditable does not require that it actuallybe audited.

a) TRUE.
b) FALSE.